VITA Virginia Information Technologies Agency

Protecting Work Comp Data and Understanding Risk in the Digital Age

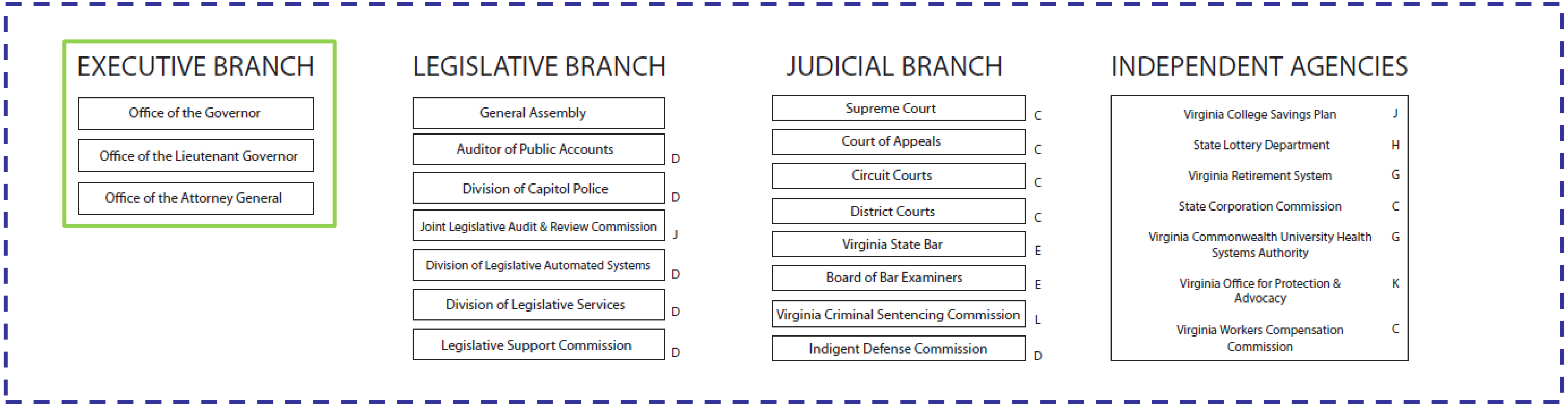
Michael Watson
Chief Information Security Officer

October 29, 2019

Overview

- Introduction
- Cybersecurity Basics
- Discussing Cyber Risks
- Reporting Cyber Threats and Risk

Information security in the commonwealth



EXECUTIVE BRANCH

- Office of the Governor
- Office of the Lieutenant Governor
- Office of the Attorney General

LEGISLATIVE BRANCH

- General Assembly
- Auditor of Public Accounts D
- Division of Capitol Police D
- Joint Legislative Audit & Review Commission J
- Division of Legislative Automated Systems D
- Division of Legislative Services D
- Legislative Support Commission D

JUDICIAL BRANCH

- Supreme Court C
- Court of Appeals C
- Circuit Courts C
- District Courts C
- Virginia State Bar E
- Board of Bar Examiners E
- Virginia Criminal Sentencing Commission L
- Indigent Defense Commission D

INDEPENDENT AGENCIES

- Virginia College Savings Plan J
- State Lottery Department H
- Virginia Retirement System G
- State Corporation Commission C
- Virginia Commonwealth University Health Systems Authority G
- Virginia Office for Protection & Advocacy K
- Virginia Workers Compensation Commission C

⬚ VITA is tasked with security governance of all three branches of commonwealth government.

□ VITA controls the infrastructure of the executive branch agencies. Agencies remain responsible for application management.

Commonwealth IT infrastructure

Computers

59,374 PCs

3,356 servers

Mailboxes

58,948 accounts

Data storage

1.5 petabytes

Mainframe

Unisys

Communications

55,000 desk phones

6,100 handhelds (PDAs)

11,000 cell phones

Networks

2,039 circuits

Data Centers (2)

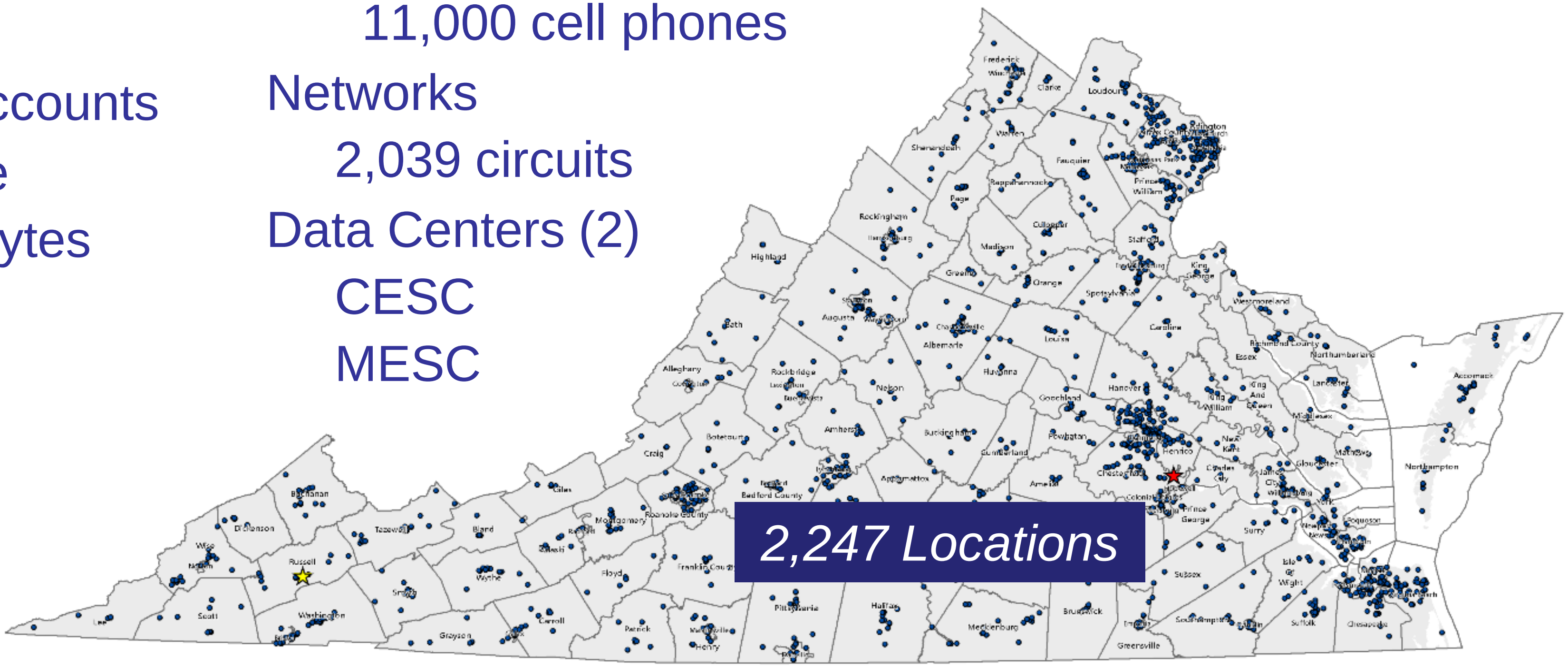
CESC

MESC

Printers

5,311 network

22,000 desktop



2,247 Locations

Cybersecurity basics

- Cybersecurity is a risk-based discipline
  - Understanding risk terminology
  - Quantifying risk
- Information security programs manage risk
  - Includes compliance requirements
  - Generates the information for the board room
- Leaders are held accountable for risk
  - Need to be aware of the cyber risk state

Classifying cybersecurity risk

Confidentiality

Integrity

Availability

Common cyber attack motivators

Financial gains

Social agenda

Cyber espionage

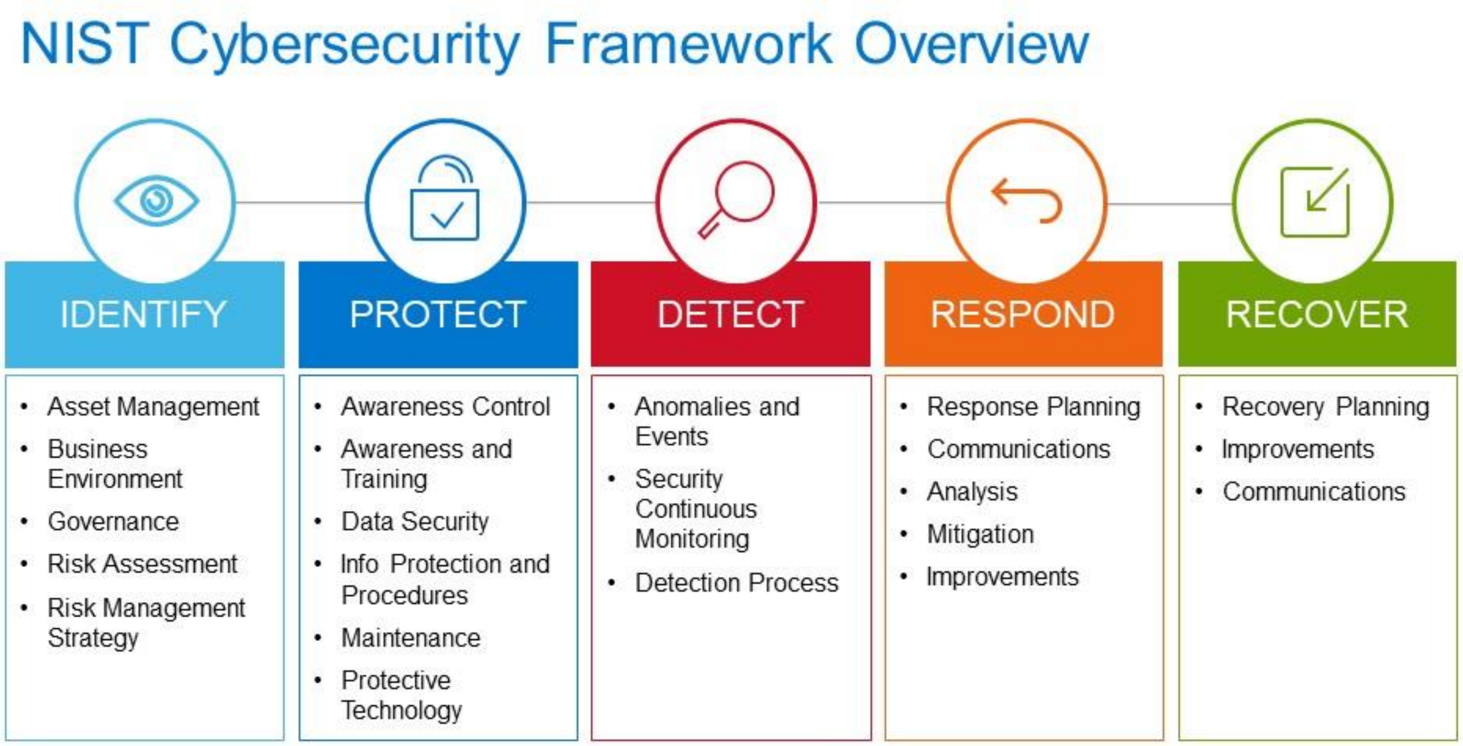
Preparing to discuss cyber risks

- Cyber objectives should address risk priorities
  - Plan for the security program to address areas of concern

- Compromise will happen eventually
  - Plan and prepare for what a compromise looks like

- Threats evolve constantly
  - Continual investment is required for adequately performing protection

Identifying cybersecurity risk



NIST Cybersecurity Framework Overview

IDENTIFY
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT
- Awareness Control
- Awareness and Training
- Data Security
- Info Protection and Procedures
- Maintenance
- Protective Technology

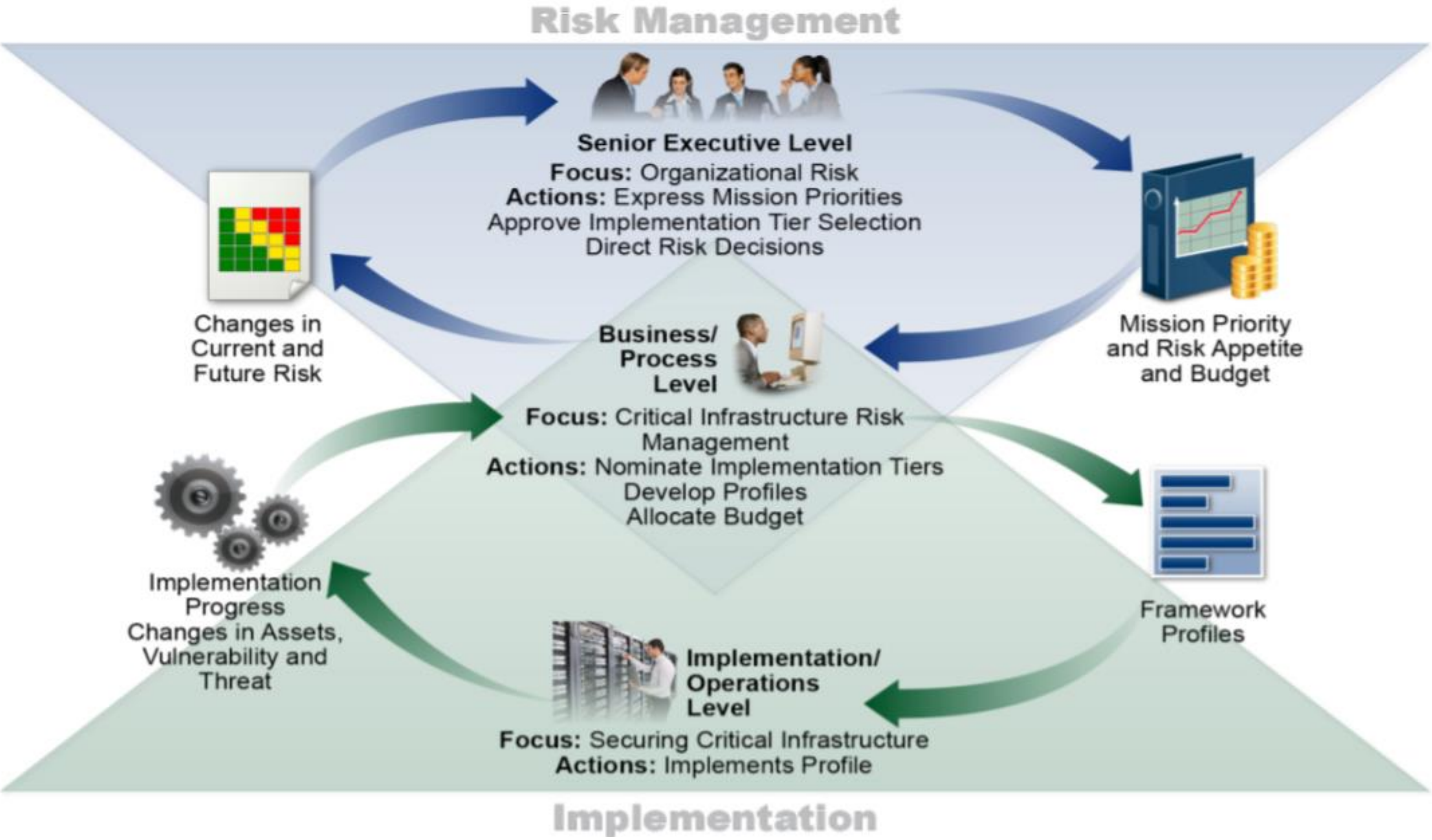
DETECT
- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

RESPOND
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Recovery Planning
- Improvements
- Communications

- Identify critical issues and concerns
  - Often standard industry issues
    - Reputation, financial, life, safety, etc.
- What amount of risk does the organization want to take on?
  - High, medium, low, etc.
- What level of risk certainty?
  - Quantitative vs. qualitative
- What risk threshold should trigger notification?
  - Investigate in four hours or 240 hours?
- What is the acceptable loss exposure?

Reporting cyber risk


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

- How sure is the organization that risks causing undesired outcomes are mitigated?
- What investments are possible to help mitigate risk?
- Are there any security events severe or potentially severe?

Questions?